AMENDMENTS TO THE SPECIFICATION

Please substitute the following corrected paragraph for its original on page 4, starting on line 16 and ending on line 32:

FIG. 4 illustrates the flow of a typical 3GPP AKA mechanism. When MS 130 requests service from SN 120, SN 120 sends (step 202) an authentication request to HE [[130]] 110. Upon receiving the request associated with a particular MS 130, HE 110 generates (step 204) an array of AVs for that particular MS 130. HE 110 sends (step 206) the AVs to SN 120 which, in turn, stores (step 208) the AVs in its Visitor Location Register (VLR). SN 120 selects (step 210) the first sequential AV(i) (e.g., i = 1) and sends (step 212) RAND(i) and AUTN(i) to MS 130. MS 130 verifies (step 214) AUTN(i) and computes RES(i). If SQN(i) is greater than SQN_{MS}, MS 130 successfully authenticates SN 120. MS 130 sends (step 216) RES(i) to SN 120. SN 120 compares (step 218) RES(i) with XRES(i). If RES and XRES are equal, SN 120 has successfully authenticated MS 130. Finally, MS 130 computes (step 220) CK(i) and IK(i) while SN 120 selects CK(i) and IK(i).

Please substitute the following corrected paragraph for its original on page 12, starting on line 22 and ending on line 30:

The optional 3GPP AKA can include procedures that allow for primitive negotiation, for example, between the HE 110 and SN 120. For example, a one byte MODE field can store data identifying the AKA cryptographic primitive or set of AKA cryptographic primitives offered by an HE 110, SN 120, or MS [[120]] 130. For example, a MODE field value of "S" can represent a request for communication using a shared SHA-1 primitive. The SN 120 authentication data requests can also include a primitive version identifier.

Please substitute the following corrected paragraph for its original starting on page 15, line 27 and ending on page 16, line 7:

The HE 110 may pass one or more AVs to SN 120 with the MODE value indicating standard 3GPP AKA. The SN 120, however, after the initial standard AKA setup, can use a common AKA primitive MODE value (e.g. SHA-1) to notify the MS 130 to use SSK and TSQN when utilizing the modified 3GPP AKA. Prior to initiating the optional AKA scheme, the SN 120 may determine if the MS 130 supports (e.g., includes instructions for) the optional scheme, for example, based on MS 130 identification information transmitted by the MS [[120]] 130. Additionally, the MS 130 can transmit a message to the SN 120 declining use of the optional scheme, for example, if the MS 130 does not provide the primitive identified by the SN 120 in the MODE field.

Please substitute the following corrected two consecutive paragraphs for their originals starting on page 17, line 26 and ending on page 18, line 12:

As shown in FIG. 14, MS 130 straddles between areas served by two different serving networks. MS 130 uses $SSK_{SN\text{-}A}$ for service from serving network A (SN-A) and $SSK_{SN\text{-}B}$ for service from serving network B (SN-B). The MS 130 may store identification of a SN and the respective SSK/TSQN pair being used. Thereafter, the MS 130 may identify the SN 120 providing service to retrieve the appropriate pair.

SSK freshness depends on the SN 120 VLR and MS 130 rules. For example, the SN 120 may [[chose]] choose to store SSK for up to a week of inactivity. The MS 130 may store multiple SSK/TSQNs in a queue (five pairs or more) using first-in-first-out (FIFO). This technique may be ideal for travelers moving between multiple systems and countries within a brief period of time. In the event the MS 130 deletes $SSK_{SN\text{-}A}$ before SN-A deletes $SSK_{SN\text{-}A}$, the MS will recognize that SN-A is attempting the optional 3GPP AKA (e.g., MODE = SHA-1), issue a user authentication reject, and await standard 3GPP AKA to establish a new SSK with SN-A.

Please insert the following GLOSSARY OF ACRONYMS on page 1, line 23, immediately after the sub-heading "Description of Related Art" to enhance clarity of presentation of the application:

--Prior to discussion of Related Art, the following Glossary of acronyms used in this specification is provided as a convenience to the reader. The acronyms are defined in the specification as they are used.

GLOSSARY OF ACRONYMS

AK - Anonymity Key
AKA - Authentication and Key Agreement
A-TK - Authentication Based on Temporary Key
AUTN - Authentication Token
AV - Authentication Vector
CK - Cipher Key
3GPP - Third Generation Project Partners
GSM - Global System Mobile
HE - Home Environment
IK - Integrity Key
K - Secret Key
KT Temporary Key
LESA - Long Term Enhanced Subscriber Authentication
MAC - Message Authentication Code
MD5 - Message Digest Algorithm 5
MS - Mobile Station
RAND Random Challenge
RES - Response
R_M - Second Random Number
R_N - Random Number
SHA - Secure Hash Algorithm
SN - Serving Network
SQN - Sequence Number
SSD - Shared Secret Data
SSK - Shared Secret Key
SSAV - Shared Secret Authorization Vector
TAUTN - Temporary Authentication Token
TIA - Telecommunication Industry Association
TSQN - Temporary SQN
USIM - Universal Subscriber Identity Module
VLR - Visitor Location Register
XRES - Expected Response--